Committee on
HOMELAND SECURITY
Chairman Peter T. King

Opening Statement

December 6, 2011

Media Contact: Shane Wolfe

(202) 226-8417

Statement of Chairman Dan Lungren (R-CA)
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
"Hearing on Draft Legislative Proposal on Cybersecurity"

December 6, 2011
Remarks as Prepared

Top government, intelligence, and military leaders point to cybersecurity as the issue that worries them the most because it touches every aspect of American life, including our military operations. Tomorrow is December 7th, a date recalled by former CIA Director Leon Panetta in recent testimony before Congress about his fear of a "cyber Pearl Harbor".

The growing connectivity between information systems, the internet, and our critical infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, and our financial networks.

We hear every day that cyber attacks are escalating around the world but particularly in the U.S., where our extensive digital networks and information systems provide a rich target for thieves and rogue nations. Disgruntled employees, hackers and even foreign governments "are knocking on the doors of these systems, and there have been intrusions". There has also been a 40% spike in cyber threats to government networks in the last year alone.

The Commerce Department estimates that the theft of intellectual property, most stolen via electronic means, costs $250 billion annually and eliminates approximately 750,000 U.S. jobs.

Cyber theft, unfortunately, is no longer our only concern. The Stuxnet Virus demonstrates an offensive capability to attack and incapacitate critical infrastructure. This presents a more immediate destructive threat - a digital warhead delivered through the internet.

Cybersecurity is now recognized as a critical component of our country's economic and national security. Failure to improve our cyber defenses will expose our intellectual property to continued theft and damage to our critical infrastructure, putting in jeopardy our future economic prosperity.

Congress needs to act to improve our cyber defenses by designating the responsible agency in government to coordinate defense of the government networks. We agree with the Administration that the Department of Homeland Security is the appropriate agency to lead this effort and protect our critical information infrastructure. My bill codifies DHS's cyber roles and responsibilities.

We need to improve our ability to assess cyber risks and strengthen cyber standards generally, with help from NIST. We should also encourage existing regulators to improve the cyber standards for the most critical infrastructure within their purview.

The cyber threat must be addressed in partnership with the private sector which owns most of the country's critical infrastructure. This will require establishing "a true trusted partnership" between government and the private sector. My objective is to create a partnership of equals designed to facilitate the exchange of cyber information and intelligence to accelerate cyber threat identification and remedies. This trusted partnership will be known as the National Information Sharing Organization.

These changes proposed in our legislation are within our Committee's jurisdiction and will enhance the cybersecurity of our critical information infrastructure.

Today's hearing will afford our private sector partners another opportunity to weigh in on our approach to protecting critical information infrastructure from this escalating cyber threat. I look forward to hearing your comments.